20-MJ-6559-MPK
20-MJ-6561-MPK

AFFIDAVIT OF SPECIAL AGENT TIMOTHY TABER IN SUPPORT OF APPLICATIONS FOR A CRIMINAL COMPLAINT AND A SEARCH WARRANT

I, Timothy Taber, being duly sworn, hereby depose and state as follows:

1. I am a Special Agent ("SA") with the United States Department of Homeland Security, Homeland Security Investigations ("HSI"), and have been so since May 2018. I have received formal training in conducting criminal investigations at the Federal Law Enforcement Training Center in Glynco, Georgia. Prior to becoming a SA with HSI, I was an Intelligence Analyst with the Federal Bureau of Investigation for approximately ten years. I am currently assigned to the HSI Boston, Massachusetts Document and Benefit Fraud Task Force ("DBFTF"), which is comprised of law enforcement agents and officers from federal, state, and local agencies. As part of the DBFTF, I am responsible for conducting investigations involving but not limited to the manufacturing, counterfeiting, alteration, sale, and use of identity documents and other fraudulent documents to evade immigration laws or for other criminal activity. Due to my training and experience, as well as conversations with other law enforcement officers, I am familiar with the methods, routines, and practices of document counterfeiters, vendors, and persons who fraudulently obtain or assume false identities.

2. The DBFTF is currently investigating a group of suspects who are believed to have obtained stolen identities of other United States citizens from Puerto Rico. Many of these individuals used the stolen identities to open bank accounts and/or credit cards to fraudulently purchase, register, and/or export vehicles as part of a multi-state scheme involving financial fraud, auto theft, and the exportation of stolen goods.

3. I am submitting this affidavit in support a criminal complaint charging Wanda SANCHEZ ("SANCHEZ") with false representation of a social security number, in violation of 42 U.S.C. § 408(a)(7)(B); aggravated identity theft, in violation of 18 U.S.C. § 1028A; and wire fraud, in violation of 18 U.S.C. § 1343.

4. I also submit this affidavit in support of an application for a search warrant for the following property: 431 Howard Street, Lawrence, Massachusetts (the "Target Location"), as described more fully in Attachment A. I have probable cause to believe that this property contains evidence, fruits, and instrumentalities of the Target Offenses, as described in Attachment B.

5. The facts in this affidavit come from my personal involvement in this investigation, including interviews of witnesses, and my review of documents and bank records, as well as my conversations with other members of law enforcement. In submitting this affidavit, I have not included every fact known to me about this investigation. Instead, I have only included facts that I believe are sufficient to establish probable cause.

Background of Investigation

6. Since approximately January 2019, HSI special agents have been investigating a scheme involving the use of stolen identities to fraudulently open bank accounts and credit cards and to purchase vehicles, many of which are then exported out of the United States. More specifically, the investigation has revealed several individuals using the stolen identities of United States citizens from Puerto Rico to fraudulently finance late-model vehicles from dealerships in Massachusetts with zero dollars down. At the dealerships, the individuals provide a variety of common identification and credit-related documents, including Puerto Rico driver's licenses and social security cards as proof of identification. The perpetrators of this fraudulent

scheme typically do not make down payments or subsequent payments on the vehicles, resulting in the dealership or relevant lending financial institution taking a total loss for the vehicles. The individuals have also been successful in opening bank accounts in the same stolen identities prior to fraudulently purchasing the vehicles. Individuals perpetrating the scheme max out associated credit cards within days or weeks and rarely make any payments on the accounts.

Probable Cause

The Credit Application

7. On or about January 16, 2019, a man and a woman appeared in person a car dealership in Boston, Massachusetts (the "Boston Dealership"). The woman provided personal identifying information on a credit application in order to purchase a 2018 Honda Odyssey (VIN: xxxxxxxxxxxxx4174) for $50,962 with 100% financing. On the credit application, the applicant represented herself as N.T.U.[1] with a date of birth of xx/xx/1973 and social security number xxx-xx-0115. The applicant listed her address as 696 N Main Street, Apartment 6, Fall River, MA, listed her occupation as the managing director of "Tirado Beauty Supply," and stated that she earned a monthly salary of $17,300. During the attempted purchase, the individual presented Puerto Rico Driver's license # 7230284 as proof of identification. The document listed the name N.T.U. with date of birth xx/xx/1973 and displayed a photograph of a woman matching the appearance of SANCHEZ.[2] After obtaining the Registry of Motor Vehicles photograph associated with the Massachusetts driver's license of SANCHEZ and comparing that photograph

[1] The identity of victim N.T.U. is known to the government. In order, these initials represent the victim's first name, paternal last name, and maternal last name. To protect the victim's privacy, only the initials "N.T.U." are used in this affidavit to reflect the victim's full name that was used by SANCHEZ.
[2] The dealership made a copy or scan of this driver's license and maintained it in its files pertaining to the transaction, which agents have reviewed.

to the photograph on the fraudulent Puerto Rico driver's license, agents determined that both photographs depict SANCHEZ.

8. That same day, the dealership submitted the personal information from the credit application over the internet via Dealertrack (described further below) to various banks for credit approval. The woman purporting to be N.T.U. was approved by a financing company located in Sacramento, CA (the "Sacramento Financing Company") on January 16, 2019 to finance the vehicle in the amount of $50,962 for a term of 72 months and that approval was communicated to the dealership via Dealertrack over the internet.

Financial Interview at the Boston Dealership

9. On May 1, 2020, an HSI agent interviewed the general manager at the Boston Dealership about the process of obtaining credit. The general manager explained that after a customer fills out all required information on the credit application, the information is manually entered into a local system called "CDK." CDK is a system the dealership uses to pull a customer's credit. Once they pull the credit, they "work the numbers" and make a deal with the customer. The credit application is then forwarded to the finance manager who manually types the information off the application into a web-based platform called "Dealertrack."[3] DealerTrack functions as a middleman by forwarding/filtering credit information from a dealership to various banks for credit approval. The general manager explained that the

[3] During the investigation, agents learned that Dealertrack is a software-as-a-service used by many automobile dealerships. It offers a single cloud-based platform to bring together consumer, dealer, and lender, and provides electronic pathways for communication between them. Dealertrack can run credit checks, submit credit applications, communicate responses, complete deals, and speed up trade-in payoff and title release. Dealertrack has a partnership with the National Credit Services Bureau. When dealers input the data and request information via the Dealertrack portal, the data is sent through a pipeline to the services cloud space where its servers are being hosted. Essentially, it is a central hub to consolidate and request all data needed for a transaction, instead of going through each individual system. Dealertrack's servers that handle this data are located in New Jersey, and have been so located since at least July 2018; accordingly, all communications between dealerships in Massachusetts and any other parties using the Dealertrack system have traveled in interstate commerce.

dealership chooses which banks they wished to request approval from and then electronically submits the customer's information to them. At that point, the selected banks receive the customer's information simultaneously and subsequently decide on approval or disapproval.

Confirmation of Valid Social Security Number; Identification of the Victim

10. The Social Security Administration ("SSA") has confirmed that social security number xxx-xx-0115 is assigned to N.T.U, a United States citizen from Puerto Rico.

11. Law enforcement contacted the Puerto Rico Police Department to obtain the driver's license of N.T.U. with social security number xxx-xx-0115. The Puerto Rico driver's license for N.T.U. listed the name N.T.U. and social security number xxx-xx-0115, but a different date of birth (xx-xx-1973) and driver's license # (xxx3036) than what was presented at the Boston Dealership in January 2019. The document also displayed the photograph of a woman who I believe to be the real N.T.U. who is different in appearance than the woman displayed in the fraudulent N.T.U. Puerto Rico driver's license presented at the Boston Dealership.

Knowledge and Use of Stolen Identity Information and Fraudulent Identification Documents

12. During sale negotiations at the Boston Dealership, due to the applicant's possession of an out of state license (Puerto Rico), the applicant was required to provide proof of residency through utility bills or other forms of documentation. The applicant provided a December 2018 National Grid bill with account number xxxxx-x4838 and an amount due of $244.08. The applicant was ultimately approved for the sale and was instructed to return later to take possession of the vehicle. On January 19, 2019, the same man who accompanied the applicant on the first visit to the dealership returned to the Boston Dealership to take possession of the vehicle. Prior to his arrival, the Boston Dealership learned of an attempted fraudulent

vehicle purchase by a different woman at a car dealership in Burlington, MA. The Boston Dealership obtained documents from the dealership in Burlington, including a National Grid bill which depicted the same account number, meter reading, meter number, and amount due as the utility bill the woman purporting to be N.T.U. presented, but a different name and address. The Boston Dealership then contacted the Boston Police Department, as they immediately suspected fraud. When the man returned to the dealership to take possession of the vehicle, officers approached him, and he was questioned. The man presented a fraudulent Puerto Rico driver's license (#8718354) in the name of C.R.R.[4] and stated that his girlfriend had instructed him to pick up the vehicle. He ultimately admitted his true name to be Ricardo ACEVEDO, and he was arrested for various forgery violations, as well as larceny over $1200 by false pretense. A fake Puerto Rico driver's license and social security card in the name of C.R.R. were found in ACEVEDO's possession and photographed by the Boston Police Department.

13. On January 15, 2020, now-Chief U.S. Magistrate Judge M. Page Kelley signed a search and seizure warrant for a black iPhone (Model A1778) that was seized from a fraudulently-purchased 2018 Jeep Grand Cherokee that was recovered with Alvin RIVERA in the driver's seat on January 17, 2019, in Methuen. After a thorough search of the phone, DBFTF agents established the phone belonged to RIVERA, a target of this investigation. Within the phone was a substantial amount of evidence which revealed RIVERA played a role in obtaining stolen identities and producing false documents to be used by his co-conspirators for fraudulent vehicle purchases. Relevant here, DBFTF agents located a PDF version of a residential lease between N.T.U. and C.R.R. Agents also located a photograph of a Puerto Rico driver's license

[4] The identity of victim C.R.R. is known to the government. In order, these initials represent the victim's first name, paternal last name, and maternal last name. To protect the victim's privacy, only the initials "C.R.R." are used in this affidavit to reflect the victim's full name that was used by Ricardo ACEVEDO.

(#8718354) in the name of C.R.R. which bore the photograph of ACEVEDO. RIVERA's phone also contained an ID card-style photograph of ACEVEDO that appeared on that driver's license. Additionally, an ID card-style photograph of SANCHEZ was located in RIVERA's phone that matched the photograph that appeared on the N.T.U. Puerto Rico driver's license that was presented at the Boston Dealership in January 2019. Agents located over 40 leases within RIVERA's phone where the date, owner, leaseholder, and address were different, but where the rest of the document was nearly identical. On certain occasions, DBFTF agents recovered copies of these leases from dealerships in Massachusetts, as "customers" had presented the documents as proof of residence during the fraudulent purchase of vehicles. Based on the above information, I believe that RIVERA assisted ACEVEDO and SANCHEZ in obtaining fraudulent documents which they subsequently used for the attempted vehicle purchase at the Boston Dealership.

14. Agents also recovered WhatsApp communications related to the N.T.U. identity between "Wandaaaa" (SANCHEZ) at 978-853-8687[5] and "$ Chapi Chapeo" (RIVERA)[6] at 978-764-7495. RIVERA sent the following message to SANCHEZ on January 2, 2019, containing the true N.T.U.'s information:

> N.T.U.
> Aptado XXX, Vega Baja, PR 00694
> DOB: xx/xx/1973
> AGE: 45
> SSN: xxx-xx-0115
> C/S: 785
> Experian Login:
> Username: nt787pr1
> Password: Cxxxxxxxxxx11

[5] Agents concluded that "Wandaaa" was Wanda Sanchez based on the similarities in the name, as well as the fact that the MA driver's license photograph of SANCHEZ matched the photograph on the fraudulent N.T.U. Puerto Rico driver's license presented at the Boston Dealership in connection with the fraudulent purchase in the N.T.U. identity.

[6] Agents were able to identify $ Chapi Chapeo $ as RIVERA, based on communications within RIVERA's iPhone in which the $ Chapi Chapeo $ user was referred to by RIVERA's name, and based on "selfie" photos he sent others from the $ Chapi Chapeo $ account, which depict RIVERA.

RIVERA sent the following message to SANCHEZ on January 5, 2019, containing some actual and some made-up biographical details for the N.T.U. identity, which SANCHEZ later used in the attempted purchase at the Boston Dealership.

N.T.U.
345 Old Whitfield St, Guilford, CT 06437-3446
Monthly Rent: $950
Been in Residence: 5Y 4M
DOB: xx/xx/1973
AGE: 45
SSN: xxx-xx-0115
Email: tiradobeautysupply@gmail.com
Phone # (475) 292-9442

15. Based on my review of RIVERA's phone, the above messages, and my training and experience, I believe that RIVERA provided SANCHEZ the stolen identity information that was used at the Boston Dealership in January 2019. The ID card-style photograph of SANCHEZ located on RIVERA's iPhone above appeared on at least two separate fraudulent Puerto Rico driver's licenses discovered in RIVERA's iPhone, for two separate stolen identities. Additionally, much of the information in the Whatsapp message sent from RIVERA to SANCHEZ on January 5, 2019 was used on the credit application SANCHEZ filled out at the Boston Dealership.

Probable Cause to Search for Evidence, Fruits, and Instrumentalities of the Target Offenses at the Target Location

16. Based on information learned in the investigation to date, including the information set forth below, there is probable cause to believe that SANCHEZ lives at and/or conducts her criminal activity from the Target Location.

17. On March 12, 2020, DBFTF agents conducted a ruse at the Target Location. A Postal Inspector observed the mailbox, located next to the front door, which listed numerous

names, including SANCHEZ. The Postal Inspector knocked on the front door and said he had a package for SANCHEZ. The Postal Inspector received verbal confirmation from SANCHEZ's mother that SANCHEZ resided at the Target Location.

18. On August 18, 2020, DBFTF agents conducted surveillance at the Target Location and, at approximately 2:50 pm, agents observed SANCHEZ on the front lawn of the Target Location.

19. I know based on my training and experience, that:

a. Individuals often keep identification documents and financial records for long periods – sometimes years – and tend to retain such documents even when they depart a given residence. Such documents include driver's licenses, social security cards, bank cards, credit cards, bank records, and credit card statements.

b. Individuals often keep identification documents and financial records in their residence, in part to ensure the security of these documents and in part to allow for access to these documents when needed.

c. In addition, it is common for those who use other persons' identities without authorization to maintain fraudulently obtained identification documents in secure locations within their residence to conceal them from law enforcement authorities;

d. It is common for individuals who use fraudulently obtained identification documents to retain those documents for substantial periods of time so that they can continue to use the fraudulently obtained identities; and

e. Based on my experience and training, I also know individuals who make purchases of goods and services often retain their receipts and invoices in their residence.

Conclusion

20. Based on the foregoing, I submit that there is probable cause to believe that, on or about January 16, 2019, WANDA SANCHEZ (1) falsely represented, with intent to deceive and for any purpose, a number to be the social security account number assigned by the Commissioner of Social Security to her, when in fact such number is not the social security account number assigned by the Commissioner of Social Security to her, all in violation of 42 U.S.C. § 408(a)(7)(B); (2) knowingly transferred, possessed and used, during and in relation to any felony violation enumerated in 18 U.S.C. 1028A(c), and without lawful authority, a means of identification of another person in violation of 18 U.S.C. § 1028A; and (3) having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises, did transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing the scheme

to defraud, to wit, stolen identity information to the Sacramento Financing Company in an attempt to secure $50,962.00 to finance a car purchase, in violation of 18 U.S.C. § 1343.

Signed under the pains and penalties of perjury this 9th day of September, 2020.

/s/ Timothy Taber

Timothy Taber
Special Agent
Homeland Security Investigations

Subscribed and sworn to via telephone in accordance with Federal Rule of Criminal Procedure 4.1 this 9th day of September, 2020.

HONORABLE M. PAGE KELLEY
CHIEF UNITED STATES MAGISTRATE JUDGE
DISTRICT OF MASSACHUSETTS

20-MJ-6561-MPK

ATTACHMENT A
Premises To Be Searched

The location to be searched is 431 Howard St, Lawrence, MA, a unit within a white multifamily home with blue trim, that has the number 431 located next to the front door and on the mailbox. Photographs of the exterior of the home are attached.

Front View of 431 Howard St, Lawrence, MA

20-MJ-6561-MPK

ATTACHMENT B
EVIDENCE TO BE SEARCHED FOR AND SEIZED

Evidence, fruits, and instrumentalities of violations of 42 U.S.C. § 408(a)(7)(B), 18 U.S.C. § 1028A, or 18 U.S.C. § 1343 (the "TARGET OFFENSES"), including but not limited to:

1. Any government-issued or apparently government-issued identification documents, notes, statements, and/or receipts that reference same;
2. Any fraudulent, stolen, or apparently fraudulent or stolen identification documents, as well as any records and communications relating to same, and any tangible items used to create or modify any identification documents;
3. Any fraudulent, stolen, or apparently fraudulent or stolen credit cards, bank cards, and records, communications, and other documents related to the same, and any tangible items used to create or modify any credit or bank cards;
4. Bank records and credit card records from January 1, 2018 to the date of execution of the warrant;
5. Records, communications, and other documents relating to the purchase or attempted purchase, financing, insuring, registration, titling, re-titling, and/or sale of any automobile and/or other vehicle, as well as funds relating to same;
6. Records, communications, and other documents relating to the movement, shipment, or export of any automobile and/or other vehicle, as well as funds relating to same;
7. Records, communications, and other documents relating to any alias or imposter identity used to purchase or attempt to purchase any automobile and/or other

vehicle; identification documents, credit or bank cards, or other records in the name(s) of such aliases; and/or any records relating to other accounts in the name(s) of such aliases;

8. Records relating to any purchase, sale, or other transaction conducted in any alias or imposter identity, or any account opened up under an alias or imposter identity;

9. Communications with any individual involved with committing and/or conspiring to commit any of the TARGET OFFENSES;

10. Communications with any individual who participated in the planning or execution of any purchase, sale, or other transaction conducted in any alias or imposter identity, or who participated in the opening or use of any account opened under an alias or imposter identity;

11. Receipts and other records relating to the expenditure of funds associated with any purchase, sale, or other transaction conducted in any alias or imposter identity;

12. Records relating to any of the proceeds derived from any of the TARGET OFFENSES, including records showing the receipt, transfer, spending, or use of such proceeds;

13. Records and tangible objects relating to the ownership, occupancy, control, or use of the premises to be searched (such as utility bills, phone bills, bank statements, rent payments, insurance documentation, receipts, check registers, and correspondence);

14. Records and tangible objects relating to the ownership, control, or use of any vehicle, phone, or other device used in furtherance of any of the TARGET

OFFENSES; and

15. Bulk cash and high-value items believed to be the proceeds or fruits of fraudulent credit card transactions or stolen car sales.